Siobhan McGreal, CSB #282196
James A. Francis (*Pro Hac Vice admission forthcoming*)
FRANCIS MAILMAN SOUMILAS, PC
1600 Market Street, Suite 2510
Philadelphia, PA 19103
T: (215) 735-8600
F: (215) 940-8000
jfrancis@consumerlawfirm.com
smcgreal@consumerlawfirm.com

Joseph C. Kohn
William E. Hoese
Zahra R. Dean (*Pro Hac Vice admission forthcoming*)
Elias A. Kohn (*Pro Hac Vice admission forthcoming*)
KOHN, SWIFT & GRAF, P.C.
1600 Market Street, Suite 2500
T: (215) 238-1700
F: (215) 238-1968
jkohn@kohnswift.com
whoese@kohnswift.com
zdean@kohnswift.com
ekohn@kohnswift.com

Kevin Laukaitis (*Pro Hac Vice admission forthcoming*)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

UNITED STATES DISTRICT COURT CENTRAL DISTRICT OF CALIFORNIA

WILLIAM YARBOUGH, PATRICIA MARSHALL, and ELIZABETH QUINBY, on behalf of themselves and all others who are similarly situated, Plaintiffs, v.	:
TICKETMASTER, LLC., LIVE NATION ENTERTAINMENT, INC., and SNOWFLAKE, INC. Defendants.	:

CLASS ACTION COMPLAINT

Plaintiffs William Yarbough, Patricia Marshall, and Elizabeth Quinby (collectively, "Plaintiffs") individually and on behalf of all others similarly situated, bring this Class Action Complaint (the "Complaint"), and allege the following against Defendants Ticketmaster, LLC ("Ticketmaster") Live Nation Entertainment, Inc. ("Live Nation"), and Snowflake, Inc. ("Snowflake"), (collectively, "Defendants"), based upon personal knowledge with respect to themselves and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. Plaintiffs brings this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similar situated individuals' personal identifiable information ("PII"), including but not limited to "full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data. [The] compromised payment data includes customer names, the last four digits of card numbers, expiration dates, and even customer fraud details" (collectively, "Private Information").[1]

2. This class action arises out of the recent targeted cyberattack against Defendant Ticketmaster's Data Cloud virtual warehouse, managed by Defendant Snowflake, that enabled a third party to access Defendants' computer systems and data, resulting in the compromise of highly sensitive Private Information (the "Data Breach").[2]

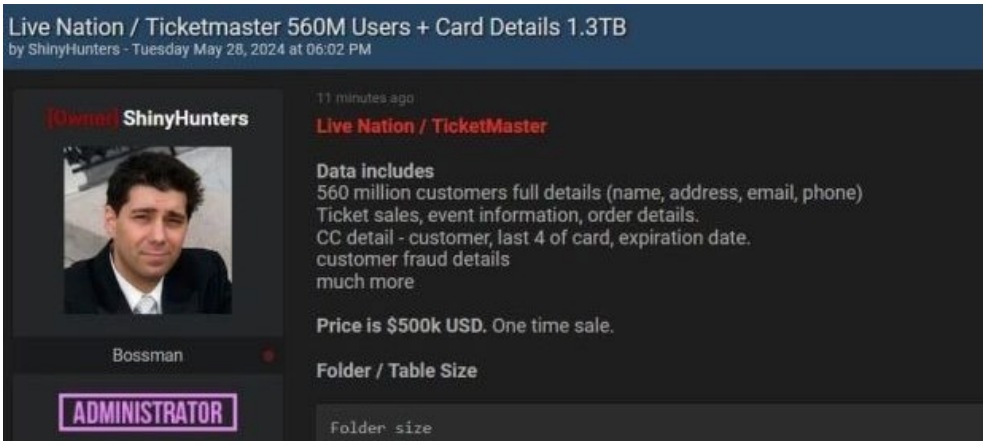
3. Due to the Data Breach, Plaintiffs and Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably

[1] Waqas, Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k, HACKREAD (May 29, 2024), https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/. (last visited July 19, 2024).
[2] *Id.*

incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their Private Information.

4. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' Private Information.

5. On or around May 28, 2024, the Private Information of 560,000,000 Ticketmaster and Live Nation's customers was compromised and listed for sale.[3]



The notorious hacker group known only by its alias "ShinyHunters" claimed that it had stolen 1.3 terabytes of personal data and is reportedly ready to sell, or has already sold, such information to nefarious dark web users for $500,000, as illustrated by their post on BreachForums, a dark-web marketplace for stolen data.

6. This Data Breach occurred because Defendants collectively enabled an unauthorized third party to gain access to and obtain former and current Ticketmaster and Live Nation's customers' Private Information from Ticketmaster's systems housed by Snowflake.[4]

[3] Georgie Hewson, Home Affairs Department confirms cyber incident impacting Ticketmaster customers, ABC NEWS (May 29, 2024), customers-data-leaked/103908614. (last visited July 19, 2024).
[4] *Id.*

7. Ticketmaster and Live Nation store customer data in a virtual warehouse provided by Defendant Snowflake, a cloud data warehouse provider offering its "Data Cloud" to institutional customers to consolidate and store data.[5]

8. As stated in their own privacy policy, Ticketmaster/Live Nation recognize the heavy burden of protection and security that they bear when collecting and storing data. Ticketmaster represents and emphasizes the following:

> "We're always taking steps to make sure your information is protected and deleted securely," "[we] have security measure in place to protect your information,"[6] and "[the] security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us."

9. Customers provide their PII to Ticketmaster with the expectation that the company will take "all necessary security measures," and that its would contract with data warehouse providers who shared the belief that the security of customers' PII is "a priority."

10. Defendants' representation of "all necessary security measures" has proven false, misleading, and stands in stark contrast to their purported prioritization of information security—Defendants admittedly failed to safeguard the PII of millions of its customers and failed to implement all necessary measures to prevent information from being stolen.

11. A criminal was able to access Defendants' Data Cloud, and obtained access to the types of information that federal and state law require companies take security measures to protect, including, but not limited to: full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data including customer names, the last four digits of card numbers, expiration dates, and customer fraud details.

---

[5] Form 10-K Annual Report for Snowflake, Inc., BAMSEC, https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited July 19, 2024).
[6] Privacy Policy, TICKETMASTER, https://privacy.ticketmaster.com/privacy-policy (last visited July 19, 2024).

12. Both the hacker group and Ticketmaster have confirmed that the stolen database was hosted by Snowflake.[7]

13. Plaintiffs, and everyone affected, are now victims of identity theft—as any combination of this PII will forever subject them to being targets of cyber-attacks. The private information exfiltrated is highly substantial and will affect the victims of this data breach, Plaintiffs and the putative class, forever. Even years from now, Plaintiffs and other victims will be subject to cyber-attacks, and phishing scams.

14. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols, consistent with the industry standard, "necessary" to protect Private Information from the foreseeable threat of a cyberattack.

15. Any entity that prioritizes the security of customers' information, employing "all necessary security measures," would ensure that it and all parties it contracts with had secure procedures to access its Data Cloud environment. Defendants did not do so, electing to brazenly utilize the Snowflake Data Cloud product knowing that Ticketmaster/Live Nation administrators could not enforce Multi-Factor Authentication ("MFA").

16. MFA is a simple yet robust security system that requires more than one method of authentication from independent categories of credentials (i.e., a username/password and confirmation link sent via email). MFA is "a critical component in protecting against identity theft, and specifically against attacks related to the successful theft of passwords."[8]

---

[7] Zach Whittaker, Live Nation Confirms Ticketmaster Was Hacked, Says Personal Information Stolen in Data Breach, TECHCRUNCH (May 31, 2024), https://techcrunch.com/2024/05/31/live-nation-confirms-ticketmaster-was-hacked-says-personal-information-stolen-in-data-breach. (last visited July 19, 2024).

[8] Shane Snider, Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say, INFORMATIONWEEK (June 5, 2024), https://www.informationweek.com/cyber-

17. ShinyHunters boasted to journalists that the Data Breach was enabled by Snowflake's lack of MFA enforcement.[9] Snowflake inexplicably leaves the option to enable MFA up to individual users, so data environments can be compromised through "weak links" – users who elect to not enroll in MFA for their accounts.[10]

18. MFA administrator enforcement is the industry standard, according to Ofer Maor, cofounder and Chief Technology Officer of data security investigation firm Mitiga.[11] He notes that "most SaaS (soft-as-a-service) vendors, once deployed as an enterprise solution, allow administrators to enforce MFA… they require every user to enroll in MFA when they first login and make it longer possible for users to work without it." A data security firm's principal simply noted it is "surprising that the built-in account management within Snowflake doesn't have more robust capabilities like the ability to enforce MFA."[12]

19. Any entity employing "all necessary" data security practices and procedures would monitor for a data security breach. In other words, even if a company negligently left the "bank vault" open (as Defendants did for eleven days following the Data Breach), it would still have videos monitoring the bank vault, and alarms that would go off if intruders tried to leave with the loot. However, Defendants failed to implement many standard monitoring and alerting systems, evinced by Defendant's inaction in the eight days following the data breach. In Live Nation's recent May 31, 2024, filing with the SEC, it confirmed that the Data Breach occurred on May 20, 2024.

---

resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say. (last visited July 19, 2024).

[9] *Id.*

[10] FAQ: Multi-Factored Authentication (MFA), SNOWFLAKE (August 5, 2023), https://community.snowflake.com/s/article/MFA-FAQs. (last visited July 19, 2024).

[11] Solomon Klappholz, With Hundreds of Snowflake Credentials Published on the Dark Web, It's Time for Enterprises to Get MFA in Order, ITPRO (June 7, 2024), https://www.itpro.com/security/cyber-attacks/with-hundreds-of-snowflake-credentials-published-on-the-dark-web-its-time-for-enterprises-to-get-mfa-in-order. (last visited July 19, 2024).

[12] Snider, supra note 9

20. Upon information and belief, Ticketmaster and Live Nation were aware of prior data breaches caused by compromised Snowflake environments, yet took no remedial or preemptive measures to ensure that their customers' data was protected (such as, by way of example, implementing a company-wide policy to enable MFA, or requesting that Snowflake employees with access to Ticketmaster's cloud environment enable MFA).

21. By acquiring Plaintiffs' and class members' Private Information for their own pecuniary benefit, Defendants assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class Members' Private Information against unauthorized access and disclosure.

22. Ticketmaster and Live Nation chose to host its data on the Snowflake Data Cloud, and IT professionals at Ticketmaster/Live Nation were on notice that they, as administrators of the platform, were unable to enforce MFA systems. Neither Defendant took any actions to ensure the safety of customers' PII, and instead knew that they had designed systems flawed with issues, and it was a matter of time for the systems to be breached. Recklessly, neither Defendant took any action to stop the preventable data breach. Accordingly, each Defendant shirked its duty to protect customers' and employees' information from being accessed by threat actors.

23. Defendants further had a duty to adequately safeguard this Private Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "FTC Act").

24. Defendants breached those duties and disregarded the rights of Plaintiff and the Class Members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard consumers' Private Information; failing to take available and

necessary steps to prevent unauthorized disclosure of data; and failing to follow applicable, required, and proper protocols, policies, and procedures regarding the encryption of data.

25. As a result of Defendants' inadequate security and breach of their duties and obligations, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiffs and Class Members have suffered injuries as a direct and proximate result of Defendants' conduct. These injuries include: (i) diminution in value and/or lost value of Private Information, a form of property that Defendants obtained from Plaintiffs and Class Members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiffs' and Class Members' Private Information; (v) the continued and certain increased risk that the Private Information that remains in Defendants' possession is subject to further unauthorized disclosure for so long as Defendants fail to undertake proper measures to protect the Private Information; (v) invasion of privacy and increased risk of fraud and identity theft; and (vi) theft of their Private Information and the resulting loss of privacy rights in that information. This action seeks to remedy these failings and their consequences. Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

26. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiffs' and Class Members' sensitive and confidential Private Information remains in the possession of Defendants. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft. The aggregate data compromised in

the Data Breach, taken as a whole, including but not limited to: full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data including customer names, the last four digits of card numbers, expiration dates, and customer fraud details, increases the risk of harm, making identity theft a likely outcome.

27. Defendants disregarded the rights of Plaintiffs and Class Members by, inter alia, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to properly train its staff and employees on proper security measures.

28. In addition, Defendants failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants properly monitored these electronic systems, Defendants would have discovered the intrusion sooner or prevented it altogether.

29. The security of Plaintiffs' and Class Members' identities is now at substantial risk because of Defendants' wrongful conduct as the Private Information that Defendants collected and maintained are now in the hands of data thieves. This present risk will continue for the course of their lives.

30. Armed with the Private Information accessed in the Data Breach, data thieves can commit a wide range of crimes.

31. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiffs and Class Members will incur out-of-pocket costs to purchase adequate credit

monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

32. Plaintiffs and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. And because they exposed other immutable personal details, the risk of identity theft and fraud will persist throughout their lives. 33. Plaintiffs bring this lawsuit on behalf of themselves and all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained.

33. Plaintiffs bring this lawsuit on behalf of themselves and all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained.

34. Plaintiffs, on behalf of themselves and all other Class Members, bring claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiffs and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

JURISDICTION & VENUE

1. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed

class, and at least one member of the class, including Plaintiffs, is a citizen of a state different from Defendants.

2. This Court has personal jurisdiction over Defendants because Defendants have purposefully availed themselves of the laws, rights, and benefits of the State of California. Defendants Ticketmaster and Live Nation are headquartered in California and all Defendants have engaged in activities including (i) directly and/or through its parent companies, affiliates and/or agents providing services throughout the United States in this judicial district; (ii) conducting substantial business in this forum; and/or (iii) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in California and in this judicial District.

3. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendants Ticketmaster and Live Nation are based in this District and Defendant Snowflake served as their vendor for the data. Defendants maintain Plaintiffs' and Class Members' Private Information in this District, and harmed Plaintiffs and Class Members in this District.

4. Defendant Snowflake is subject to personal jurisdiction in California based on sufficient minimum contacts which exist between Defendants Ticketmaster and Live Nation and California, and the decisions affecting consumers data privacy stored on the Snowflake Data Cloud stem from communications between Defendant Snowflake and California based Defendants Ticketmaster and Live Nation. Defendant Snowflake advertises and solicits business in California and has purposefully availed itself to the protections of California law and should reasonably expect to be hauled into court in this District.

PARTIES

Plaintiff William Yarbrough

5. Plaintiff William Yarbough is a citizen of the State of Pennsylvania. At all relevant times, he resided in Pennsylvania.

6. Plaintiff provided his PII to Defendants.

7. In receiving and maintaining his PII for its business purposes, Defendants expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Yarbrough's PII. Defendants, however, did not take proper care of Plaintiff Yarbrough's PII, leading to exposure to and exfiltration by cybercriminals as a direct result of Defendants' inadequate cybersecurity measures.

8. Plaintiff Yarbrough is deeply concerned by the Data Breach and the loss of his PII, which is now readily available for cybercriminals to sell, buy, and exchange, on the dark web.

9. Plaintiff anticipates needing to spend substantial time to determine the extent and gravity of the Data Breach and to mitigate damages. Plaintiff will need to review and closely monitor his credit reports and financial accounts for fraudulent activity.

10. Plaintiff Yarbrough suffers a substantially increased risk of fraud and identity theft resulting from his PII being stolen and leaked on the dark web and subjected to unauthorized third parties/criminals.

11. Plaintiff Yarbrough has a continuing interest in ensuring that his PII, which remains in Defendants' possession, is protected and safeguarded from future data breaches.

Plaintiff Patricia Marshall

12. Plaintiff Patricia Marshall is a citizen of the State of Vermont. At all relevant times, she resided in Pennsylvania.

13. Plaintiff provided her Private Information to Defendants.

14. In receiving and maintaining her Private Information for its business purposes, Defendants expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's Private Information. Defendants, however, did not take proper care of her Private Information, leading to exposure to and exfiltration by cybercriminals as a direct result of Defendants' inadequate cybersecurity measures.

15. Plaintiff Marshall is deeply concerned by the Data Breach and the loss of her Private Information, which is now readily available for cybercriminals to sell, buy, and exchange, on the Dark Web.

16. Plaintiff anticipates needing to spend substantial time to determine the extent and gravity of the Data Breach and to mitigate damages. Plaintiff will need to review for fraudulent activity and closely monitor her financial information.

17. Plaintiff Marshall suffers a substantially increased risk of fraud, identity theft, and data misuse resulting from her Private Information being leaked on to the Dark Web and subjected to unauthorized third parties/criminals.

18. Plaintiff Marshall has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Elizabeth Quinby

19. Plaintiff Quinby is a citizen of the State of California. At all relevant times, she resided in Pennsylvania.

20. Plaintiff Quinby provided her Private Information to Defendants.

21. In receiving and maintaining her Private Information for its business purposes, Defendants expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's Private Information. Defendants, however, did not take proper care of her Private

Information, leading to exposure to and exfiltration by cybercriminals as a direct result of Defendants' inadequate cybersecurity measures.

22. Plaintiff Quinby is deeply concerned by the Data Breach and the loss of her Private Information, which is now readily available for cybercriminals to sell, buy, and exchange, on the Dark Web.

23. Plaintiff Quinby anticipates needing to spend substantial time to determine the extent and gravity of the Data Breach and to mitigate damages. Plaintiff will need to review for fraudulent activity and closely monitor her financial information.

24. Plaintiff Quinby suffers a substantially increased risk of fraud, identity theft, and data misuse resulting from her Private Information being leaked on to the Dark Web and subjected to unauthorized third parties/criminals.

25. Plaintiff Quinby has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Defendant Live Nation Entertainment, Inc.

26. Defendant Live Nation Entertainment, Inc. is a Delaware corporation headquartered in California with its principal executive office located at 9348 Civic Center Drive, Beverly Hills, CA 90210.

27. Live Nation is one of, if not the largest, live entertainment companies in the world. Live Nation gathers, stores, and, upon information and belief, has monetized millions of customers' data. Live Nation promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements, which it failed to do.

Defendant Ticketmaster, LLC

28. Defendant Ticketmaster, LLC. is a wholly owned subsidiary of Defendant Live Nation Entertainment, Inc. which is headquartered in California with its principal executive office located at 9348 Civic Center Drive, Beverly Hills, CA 90210.

29. Ticketmaster and Live Nation Entertainment merged in January 25, 2010.

30. Ticketmaster operates as a ticket distribution company that buys, transfers, and sells tickets for live music, sporting, arts, theater, and family events and has clients worldwide. Ticketmaster requires customers to provide personally identifiable information in order to complete the purchase, even though that information is not required to complete the transaction.

31. Ticketmaster has stored this data and benefits from the accumulation and storage of this data. Data includes full names, payment information and addresses, locations, and other private and sensitive information. Ticketmaster promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements, which it failed to do.

32. Due to the nature of the services Ticketmaster provides, it receives and is entrusted with securely storing consumers' Private Information, which includes, individuals' full name, payment information, occasional location data, and other sensitive information. Ticketmaster promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

33. Plaintiffs and Class Members are current and former customers of Ticketmaster and account holders on Ticketmaster.com.

34. Defendant Snowflake, Inc. is a Delaware corporation headquartered in Montana with its principal executive office located at 106 E. Babcock, Suite A Bozeman, MT 59715.

35. this information in Snowflake's cloud computing system and storage.

Defendant Snowflake, Inc.

36. Defendant Snowflake, Inc. is a Delaware corporation headquartered in Montana with its principal executive office located at 106 E. Babcock, Suite A Bozeman, MT 59715.

37. Defendant Snowflake, Inc. is a Delaware corporation headquartered in Montana with its principal executive office located at 106 E. Babcock, Suite A Bozeman, MT 59715.

38. Snowflake is a publicly traded corporation listed on the New York Stock Exchange with revenues totaling approximately $829 million for the three months ended on April 30, 2024.[13]

39. Snowflake's Data Cloud platform is used globally, with 9,437 institutions trusting Snowflake to manage and store customers' data.[14]

40. Due to the nature of the services Snowflake provides, it receives and is entrusted with securely storing consumers' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive information. As a contracting party entrusted with millions of customers' PII, Snowflake was expected to provide confidentiality and adequate security for the data it collected in accordance with Defendant Ticketmaster's promises and disclosures and is expected to comply with statutory privacy requirements.

FACTUAL ALLEGATIONS

A. The Data Breach, and Defendants Unsecure Data Management.

[13] Form 10-Q Quarterly Report for Snowflake, Inc., BAMSEC, https://www.bamsec.com/filing/164014724000135?cik=1640147 (last visited July 18, 2024).
[14] Form 10-K Annual Report for Snowflake, Inc., BAMSEC, https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited July 19, 2024).

41. On May 28, 2024, threat actors posted that 1.4 terabytes of Private Information were available for purchase on the hacking website Breach Forums.[15] The notorious hacking group ShinyHunters offered the trove of Plaintiffs' and Class Members' Private Information for $500,000.

42. Defendants have confirmed the Data Breach occurred on May 20, 2024, noting there was "unauthorized activity within a third-party cloud database environment."[16] Such data includes, according to the hackers' forum post, "560 million customers [sic] full details (name, address, email, phone) – Ticket sales, event information, order details – CC [credit card] detail [sic] – customer, last 4 of card, expiration date. Customer fraud details – much more."[17] Defendants waited eleven days to confirm the breach.

43. Prior to the Data Breach in May 2024, Plaintiffs and Class Members had provided their Private Information to Ticketmaster with the reasonable expectation and mutual understanding that Ticketmaster would comply with its obligations to keep such information confidential and secure from unauthorized access. In particular, Plaintiffs and Class Members provided their names, emails, phone numbers, location data and credit card information to Ticketmaster in order to register for an account and purchase event tickets on Ticketmaster.com.

44. PII is a valuable property right.[18] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the

---

[15] Waqas, supra note 1.
[16] Form 8-K Current Report for Live Nation Entertainment, Inc., SEC.GOV, https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm?=7194ef805fa2d04b0f7e8c9521f97343 (last visited July 19, 2024).
[17] *Id.*
[18] See Marc van Lieshout, The Value of Personal Data, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26-38 (May 2015), https://www.researchgate.net/publication/283668023. (last visited July 19, 2024). The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

existing legal and regulatory frameworks."[19] It is estimated that American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[20] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years. Indeed, the threat actor who compromised Defendants' systems is seeking a one-time payment of half a million dollars in exchange for this Private Information.

45. Plaintiffs and the Class's Private Information exposed in the Data Breach has been exposed on the Dark Web.

46. Ticketmaster promised consumers it would keep their data secure and private. Data security is purportedly a critical component of Ticketmaster's business model. On a section of its website, Ticketmaster confidently asserts the following statements:

> "We're always taking steps to make sure your information is protected and deleted securely," "[we] have security measure in place to protect your information,"[21] and "[the] security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us."[22]

47. On its website, Ticketmaster maintains an "Our Commitments" section, including "Security & Confidentiality" as one of "10 commitments that drive [Ticketmaster's] privacy program, globally".[23]

---

[19] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD No. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en. (last visited July 19, 2024).
[20] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/. (last visited July 19, 2024).
[21] Privacy Policy, TICKETMASTER, https://privacy.ticketmaster.com/privacy-policy (last visited July 19, 2024).
[22] Our Commitments, TICKETMASTER, https://privacy.ticketmaster.com/en/our-commitments (last visited July 19, 2024).
[23] *Id.*

48. Contrary to Ticketmaster's various express assurances that it would take reasonable measures to safeguard the sensitive information entrusted to it, it chose to host customers' data on the Snowflake Data Cloud, with full knowledge that its administrators could not enforce MFA security systems, and an unauthorized, criminal element was able to access customers' data because of this decision.

49. To date, Ticketmaster has not disclosed complete specifics of the attack, such as whether ransomware has been used.

50. As such, Ticketmaster, and its parent company Live Nation, have failed to secure the PII of the individuals that provided their sensitive information. Defendants failed to take appropriate steps to protect the PII of Plaintiffs and other Class Members from being disclosed.

B. Defendants Failed to Comply with FTC Guideline

51. Defendants were prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

52. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of

personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[24] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[25]

54. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. See, e.g., In the Matter of Labmd, Inc., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

---

[24] Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited July 19, 2024).

[25] *Id.*

57. Defendants failed to properly implement basic data security practices, allowing for this attack to occur, victimizing millions of people.

58. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Defendants were at all times fully aware of the obligation to protect the Private Information of customers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

C. Plaintiffs and the Class Have Suffered Injury as a Result of Defendants' Data Mismanagement

60. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiffs and Class Members' Private Information has been and are now in the hands of an unauthorized third-party which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiffs and Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

61. Plaintiffs and Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

62. Plaintiffs and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim for cybercrimes for years to come.

63. As a result of Private Information's real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security

numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

64. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[26] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[27]

65. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

66. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[26] Anita George, Your personal data is for sale on the dark web. Here's how much it costs, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs//. (last visited July 19, 2024).

[27] Brian Stack, Here's How Much Your Personal Information Is Selling for on the Dark Web, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. (last visited July 19, 2024).

[28] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1
(last visited July 19, 2024).

67. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.[29] The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendants on notice, long before the Data Breach, that 1) cybercriminals are targeting large, public companies such as Defendants Live Nation and Snowflake; 2) cybercriminals were ferociously aggressive in their pursuit of large collections of PII like that in possession of Defendants; 3) cybercriminals were selling large volumes of PII and corporate information on Dark Web portals; 4) the threats were increasing.

68. Had Defendants been diligent and responsible, they would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key avoidable causes for data security incidents are:

a. Lack of complete assessment, including internal, third-party, and cloud-based systems and services;

b. Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;

c. Misconfigured devices/servers;

d. Unencrypted data and/or poor encryption key management and safeguarding;

e. Use of end-of-life (and thereby unsupported) devices, operating systems and applications;

f. Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;

[29] Ben Kochman, FBI, Secret Service Warn of Targeted Ransomware, LAW360 (Nov. 18, 2019), accessible at https://www.law360.com/articles/1220974 (last visited July 19, 2024).

g. Failure to block malicious email; and

h. Users succumbing to business email compromise (BEC) and social exploits.[30]

69. Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

70. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendants' conduct. Further, the value of Plaintiffs' and Class Members' Private Information has been diminished by its exposure in the Data Breach.

71. As a result of Defendants' failures, Plaintiffs and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their Private Information.

72. Plaintiffs and members of the Class suffered actual injury from having Private Information compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

[30] Gretel Egan, OTA Report Indicates 93% of Security Breaches Are Preventable, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/securityawareness/post/ota-report-indicates-93-security-breaches-are-preventable (last visited July 19, 2024).

73. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm.

74. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Private Information.

75. Plaintiffs, individually and on behalf of all other similarly situated individuals, allege claims in negligence, negligence per se, breach of implied contract, unjust enrichment, violations of the California Consumer Privacy Act, California Legal Remedies Act, and California's Unfair Competition Law.

CLASS ALLEGATIONS

76. Plaintiffs brings this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

77. The Classes that Plaintiffs seek to represent is defined as follows:

Nationwide Class

> All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of a data breach that occurred on, or about, May 20, 2024, as reported by Defendant Live Nation (the "Class").

California Subclass

> All individuals residing in California whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant Live Nation (the "Pennsylvania Subclass").

Pennsylvania Subclass

> All individuals residing in Pennsylvania whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant Live Nation (the "Pennsylvania Subclass").

Vermont Subclass

All individuals residing in Vermont whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant Live Nation (the "Vermont Subclass").

78. Collectively, the Class, California Subclass, Pennsylvania Subclass, and Vermont Subclass are referred to as the "Classes" or "Class Members."

79. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

80. Plaintiffs reserve the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

81. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time and such number is exclusively in the possession of Defendants, upon information and belief, millions of individuals were impacted in the Data Breach.

82. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

83. Typicality: Plaintiffs' claims are typical of those of the other members of the Classes because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Classes.

84. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

85. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

86. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a

complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

87. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

88. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

89. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

90. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Classes, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

91. Further, Defendants have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

92. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the Plaintiffs and the Classes of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;

c. Whether Defendants' (or their vendors') security measures to protect their network were reasonable in light of industry best practices;

d. Whether Defendants' (or their vendors') failure to institute adequate data protection measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII;

f. Whether Defendants made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and

g. Whether adherence to FTC recommendations for protecting personal information would have reasonably prevented the Data Breach

CLAIMS FOR RELIEF

COUNT I:
NEGLIGENCE
(On Behalf of Plaintiffs and the Classes against Defendants)

93. Plaintiffs re-allege and incorporate by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

94. Defendants gathered and stored the PII of Plaintiffs and Class Members as part of their business of soliciting its services to their customers. Plaintiffs and Class Members entrusted Defendants with their PII with the understanding that Defendants would adequately safeguard their information.

95. Defendants had full knowledge of the types of PII they collect and the types of harm that Plaintiffs and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

96. By collecting, storing, sharing, and using the Plaintiffs' and Class Members' PII for commercial gain, Defendants assumed a duty to use reasonable means to safeguard the personal data they obtain.

97. Defendants' duty included a responsibility to ensure they: (i) implemented reasonable measures to detect and prevent unauthorized intrusions into their network; (ii) were contractually obligated to adhere to the requirements of Defendants' privacy policy; (iii) were required to comply with the same statutes and data protection obligations as the Defendants; (iv) were required to submit to regular privacy assessments and security audits; (v) were regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) were obligated to provide timely notice to individuals impacted by a data breach event.

98. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive practices that affect commerce. Deceptive practices, as interpreted and enforced by the FTC, include failing to adhere to a company's own stated privacy policies.

99. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII they were no longer required to retain. Defendants had a duty to promptly and adequately notify Plaintiffs and the Classes of the Data Breach.

100. Defendants have a duty to adequately disclose that the PII of Plaintiffs and the Classes within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

101. Defendants breached their duties, pursuant to the FTC Act, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former customers' PII it was no longer required to retain;

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and,

g. Failing to ensure their vendors implemented data security practices consistent with Defendants' published privacy policies.

102. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

103. The injuries resulting to Plaintiffs and the Classes because of Defendants failure to use adequate security measures was reasonably foreseeable. Further, the Data Breach was reasonably foreseeable given the Defendants prior experience with cyberattacks and data breaches.

104. Plaintiffs and the Class were the foreseeable victims of a data breach. Defendants knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of protecting PII transmitted to and maintained on third party systems.

105. Plaintiffs and the Classes had no ability to protect the PII in Defendants' possession. Defendants were in the best position to protect against the harms suffered by Plaintiffs and the Classes as a result of the Data Breach.

106. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Classes, their PII would not have been compromised. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Classes and the harm, or risk of imminent harm, suffered by Plaintiffs and the Classes.

107. As a result of the Data Breach, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

108. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

109. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

110. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT II:
NEGLIGENCE *PER SE*
(On Behalf of the Plaintiffs and the Classes against Defendants)

111. Plaintiffs reallege and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

112. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive practices that affect commerce. Deceptive practices, as interpreted and enforced by the FTC, include failing to adhere to a company's own stated privacy policies.

113. Defendants violated Section 5 of the FTC Act by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiffs and Class Members information. Defendants further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII.

114. Defendants' violations of Section 5 of the FTC Act, and other state consumer protection statutes, constitute negligence *per se.*

115. Plaintiffs and Class Members are within the class of persons Section 5 of the FTC Act, and other state consumer protection statutes, were intended to protect. Moreover, the harm that has occurred is the type of harm the FTC Act, and similar state statutes were intended to guard against.

116. But for Defendants wrongful and negligent breach of duties owed to Plaintiffs and the Classes, the PII of Plaintiffs and the Class would not have been compromised.

117. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix)

nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

118. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

119. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

120. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

121. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT III:
BREACH OF IMPLIED CONTRACT
(On Behalf of the Plaintiffs and the Classes against Defendants Ticketmaster and Live Nation)

122. Plaintiffs reallege and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

123. Defendants Ticketmaster and Live Nation require their customers, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing ticketing services for live entertainment events.

124. Plaintiffs and the Classes entrusted their PII to Defendants. In so doing, Plaintiffs and the Classes entered implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiffs and the Classes if their data had been compromised or stolen.

125. Defendants promulgated, adopted, and implemented written privacy policies whereby they promised Plaintiffs and Class Members that they would (a) use PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt notice of any unauthorized access and/or theft of their PII, (e) reasonably ensure their vendors safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential

126. Plaintiffs and Class Members would not have entrusted their PII to Defendants in the absence of their implied promise to implement reasonable data protection measures.

127. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

128. Defendants breached the implied contracts it made with Plaintiffs and the Classes by failing to protect their personal information, by failing to delete the information once the relationship ended, and by failing to provide adequate notice of the Data Breach.

129. As a direct and proximate result of Defendants breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

130. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

131. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT IV:
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Classes against Defendants)

132. Plaintiffs reallege and incorporate by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

133. By providing their PII, Plaintiffs and Class Members conferred a monetary benefit on Defendants. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them and have accepted and retained that benefit. Defendants sold their PII and used the data to market and sell additional services to Plaintiffs and Class Members.

134. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

135. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, they would not have entrusted their PII to Defendants.

136. Plaintiffs and Class Members have no adequate remedy at law.

137. Under the circumstances, it would be unjust for Defendants to retain any of the benefits that Plaintiffs and Class Members conferred upon them.

138. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

139. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct.

COUNT V:
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs and the Classes against Defendants Ticketmaster and Live Nation)

140. Plaintiffs realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

141. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

142. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendants.

143. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of PII and financial information and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

144. Defendants acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT VI:
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 Cal. Civ. Code §§ 1798.100 et seq. ("CCPA") (On Behalf of the California Subclass)

145. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

146. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

147. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

148. Defendants are subject to the CCPA and failed to implement such procedures which resulted in the Data Breach. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure because of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

149. Plaintiff Quinby and the California Subclass are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are natural persons residing in the state of California.

150. Defendants are a "business" as defined by Civ. Code § 1798.140(c).

151. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." *See* Civ. Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

152. Plaintiff Quinby's Private Information compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA. Through the Data Breach, Plaintiff's private information was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

153. The Data Breach occurred because of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

154. Simultaneously herewith, Plaintiff is providing notice to Defendants pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have violated or are violating. Although a cure is not possible under the circumstances, if (as expected) Defendants are unable to cure or do not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

155. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks statutory damages of up to $750 per class member (and no less than $100 per class member), actual damages to the extent they exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VII:
VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT Cal. Civ. Code §§ 1750 et seq. ("CLRA") (On Behalf of the California Subclass, against TicketMaster and Live Nation only)

156. Plaintiff Quinby realleges and incorporates by reference every allegation contained elsewhere in this Complaint as if fully set forth herein.

157. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "**CLRA**"), California Civil Code § 1750, et seq. This cause of action does not seek monetary damages currently and is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendants with notice required by California Civil Code § 1782.

158. Plaintiff and Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

159. Plaintiff, Class Members and Defendants have engaged in "transactions," as that term is defined by California Civil Code § 1761(e) by acquiring services of Ticketmaster and Live Nation for personal and not commercial use.

160. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct undertaken by Defendants was likely to deceive consumers.

161. Cal. Civ. Code § 1770(a)(2) prohibits Live Nation and Ticketmaster from misrepresenting the source, sponsorship, approval or certification of goods or services. Both Defendants violated this provision by making commitments and promises to customers and Plaintiff specifically regarding its services, security, and privacy.

162. Cal. Civ. Code § 1770(a)(5) prohibits both Defendants (Live Nation and Ticketmaster) from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." Here, both Defendants violated this provision by misrepresenting its services as being of specific qualities, approval, and providing benefits – the promised commitments and security of customers' information. Both Defendants sold their services with the representations of security and confidentiality, none of which were truthful.

163. Similarly, Cal. Civ. Code § 1770(a)(7) prohibits both Defendants from representing their goods and services are of a particular standard, quality, or grade. Here, both Defendants misrepresented the standards and quality of their services and products, while knowing that their security, privacy policies, and processes do not meet even the industry standards, contain serious security issues, and put any customer using/purchasing Defendants' goods or services at risk of having customers' confidential information exposed.

164. Both Defendants also violated Cal. Civ. Code § 1770(a)(16) by failing to supply its goods and services in accordance with their previous representations. 158. Ticketmaster and Live Nation violated CLRA provisions by representing that they took appropriate measures to protect Plaintiff's and the Class Members' Private Information Additionally, Ticketmaster and Live Nation improperly handled, stored, or protected either unencrypted or partially encrypted data, utilized Snowflake's services while knowing of critical issues and lack of appropriate security measures in Snowflake's systems. Ticketmaster and Live Nation also failed to instruct Snowflake to implement the necessary security measures to ensure that their customers confidential information remains protected.

165. As a result, Plaintiff and the Class Members were induced to provide their Private Information to Defendants.

166. As a result of engaging in such conduct, Ticketmaster and Live Nation have violated Civil Code § 1770.

167. Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

168. Plaintiff and the Class Members suffered injuries caused by Defendants' misrepresentations, because they provided their Private Information believing that Defendants would adequately protect this information.

169. Plaintiff and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

170. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiff and members of the Class.

COUNT VIII:
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW Cal. Bus. and Prof. Code §§ 17200, et seq. ("UCL") (On Behalf of the California Subclass against Defendants)

171. Plaintiff Quinby re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

172. Plaintiff brings this claim on behalf of themselves and the California Class.

173. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("**UCL**"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

174. By reason of Defendants' above-described wrongful actions, inaction, and omission, the resulting Data Breach, and the unauthorized disclosure of Plaintiff's and Class Members' Private Information, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

175. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the private and confidential Private Information of consumers has been compromised for all to see, use, or otherwise exploit. 170. Defendants' practices were unlawful and in violation of the CCPA and CLRA and Defendants' own privacy policy because Defendants failed to take reasonable measures to protect Plaintiff's and Class Members' Private Information.

176. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the Private Information they provide to Defendants will remain private and secure, when in fact it was not private and secure.

177. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions,

inaction, and omissions including, inter alia, the unauthorized release and disclosure of their Private Information.

178. Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 et seq., in that Defendants' conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy, immoral, unethical, oppressive, and unscrupulous, and the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

179. But for Defendants' misrepresentations and omissions, Plaintiff and Class Members would not have provided their Private Information to Defendants or would have insisted that their Private Information be more securely protected.

180. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information, they have been injured as follows: (1) the loss of the opportunity to control how their Private Information is used; (2) the diminution in the value and/or use of their Private Information entrusted to Defendants; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their Private Information; and (5) costs associated with monitoring their Private Information, amongst other things.

181. Plaintiff takes upon herself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of Private Information. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiff by forcing her to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

a) For an Order certifying the Classes, and appointing Plaintiffs and her Counsel to represent the Classes;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;

c) For injunctive relief and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an Order:

i. prohibiting Defendants from engaging in the wrongful acts described herein;

ii. requiring Defendants to protect all data collected during the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to delete the PII of Plaintiffs and Class Members unless Defendants can provide a reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII they collect; and

v. requiring Defendants to audit, test, and train their vendors regarding data protection procedures.

d) For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f) For prejudgment interest on all amounts awarded; and

g) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: August 5, 2024

Respectfully Submitted,

Kevin Laukaitis (*Pro Hac Vice admission forthcoming*)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

/s/ Siobhan McGreal
Siobhan McGreal, CSB #282196
James A. Francis (*Pro Hac Vice admission forthcoming*)
FRANCIS MAILMAN SOUMILAS, PC
1600 Market Street, Suite 2510
Philadelphia, PA 19103
T: (215) 735-8600
F: (215) 940-8000
jfrancis@consumerlawfirm.com
smcgreal@consumerlawfirm.coM

Joseph C. Kohn
William E. Hoese
Zahra R. Dean (*Pro Hac Vice admission forthcoming*)
Elias A. Kohn (*Pro Hac Vice admission forthcoming*)
KOHN, SWIFT & GRAF, P.C.
1600 Market Street, Suite 2500
T: (215) 238-1700
F: (215) 238-1968
jkohn@kohnswift.com
whoese@kohnswift.com
zdean@kohnswift.com
ekohn@kohnswift.com

Attorneys for Plaintiffs and the Classes